CEESEDEN
CENTRO DE ESTUDIOS ESTRATÉGICOS SOBRE SEGURIDAD Y DEFENSA NACIONALES

Cibernética en la guerra contemporánea: definición de nuevos escenarios estratégicos y operacionales[1]

ANDRÉS GAITÁN RODRÍGUEZ[2]

Recibido:
10 de octubre de 2015

Aprobado:
04 de diciembre de 2015

Palabras claves:
Cibernética, ciberguerra, drones, información, tecnologías informáticas, ciborgs

Key words:
Cybernetics, cyberwar, drones, information, computer technologies, cyborgs.

Resumen

El presente artículo expone un concepto de ciberguerra, que más que estar descrito por el ambiente o dimensión en donde se desarrolla, este se fundamenta en la base o naturaleza misma del proceso: la cibernética. Desde este enfoque, la ciberguerra presenta características tanto cualitativas como temporales que no suelen emplearse al momento de definirla como fenómeno de la defensa nacional, así como amenaza para aquellos Estados que padecen de sus efectos. La ciberguerra no debe entenderse exclusivamente como ciberataques a infraestructura crítica o ciberespionaje ya que es una problemática que se viene configurando años atrás, pero más importante que esto, que trasciende la creación de nuevos escenarios estratégicos y operacionales a partir del principio del control que proviene de la cibernética.

Cybernetics in contemporary war: definition of new strategic and operational scenarios

Abstract

This article exposes a cyberwar concept, that besides being described by the environment or dimension where it develops, it is based in the base or nature itself of the process: cybernetics. From this approach, the cyberwar has qualitative and temporal characteristics that aren't used at the moment

1. Artículo de reflexión vinculado al proyecto de investigación "Inteligencia Tecnológica", del grupo de investigación "Centro de Investigación en Guerra Asimétrica" de la Escuela de Inteligencia y Contrainteligencia "Brigadier General Ricardo Charry Solano".
2. Magíster en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra, Colombia. Politólogo con énfasis en Relaciones Internacionales de la Pontificia Universidad Javeriana, Colombia. Asesor del Departamento de Doctrina, Ciencia y Tecnología de la Escuela de Inteligencia y Contrainteligencia "Brigadier General Ricardo Charry Solano". Contacto: andresgaro@gmail.com.

of defining it as a national security phenomenon, thereby a threat to those states that suffer from its effects. Cyberwar must not be understood exclusively as cyberattacks to critical infrastructure or cyberespionage because it's a problematic that has been setting many years ago, but even more important than this, is that it transcends the creation of new strategic and operational settings starting from the control that comes from cybernetics.

El siglo XX y lo que ha transcurrido del XXI, ha permitido el desarrollo de una gran cantidad de campos, con el objetivo de cumplir las ambiciones del ser humano, mejorar su calidad de vida y otorgarle un mayor poder en el control de su entorno. En este último aspecto, la cibernética es una disciplina muy importante, por la oportunidad que le entrega a la sociedad académica, y en general a la comunidad internacional. "La cibernética es el estudio de la interacción hombre – máquina, guiada por el principio de que los diferentes tipos de sistemas pueden ser estudiados de acuerdo a principios de retroalimentación, control y comunicaciones" (Mindell, 2000). Pero esta definición es una de las muchas que existen.

La cibernética es un concepto sobre el cual aún no existe consenso a nivel internacional, Aquí algunos de ellos: Para Andrey Kolmogorov es una ciencia que se ocupa del estudio de los sistemas de cualquier naturaleza que sean capaces de recibir, almacenar y procesar la información con el fin de utilizarla para el control (Universidad Nacional Autónoma de México, 2015). Según William Ross Ashby (1997), la cibernética se refiere a todas las formas de comportamiento en la medida en que estas sean regulares, o determinables o reproducibles. Para el británico Gregory Bateson, es una rama de las matemáticas que se ocupa de los problemas de control, recursividad e información (Sierra Agudelo, 2011, p. 51).

La elección de la palabra griega no fue al azar: "procede del griego kybernetiké perteneciente al piloto, o al arte de gobernar" (Castaño Ales, 2000). Las definiciones han sido desarrolladas por algunos de los científicos más brillantes del siglo XX. "La ciencia del control y la comunicación sobre el animal y la máquina" (Wiener, 1965), fue el concepto que construyó Norbert Wiener, quien ha sido calificado como el creador de la cibernética. El término se originó en 1947, cuando Wiener necesitaba encontrar un vocablo para nombrar una disciplina aparte, pero que incluía otros campos como la ingeniería eléctrica, las matemáticas, la biología, la neurofisiología, la antropología y la psicología.

> La palabra Cibernética deriva del griego kubernetes, que significa timonel. En este sentido la cibernética es entonces el estudio de las estructuras de los sistemas reguladores, es decir se propone develar los mecanismos presentes en los sistemas que sirven para regular los actos del "otro" o de sí mismo. Wiener se refiere al "otro" tanto para los grupos humanos como para las máquinas e instala la cibernética en el centro de la teoría de los mensajes, al querer regular el comportamiento o el actuar, tanto de una máquina como de un ser o un grupo humano. (Castro & Filippi, 2010, p. 147).

En la tesis de su libro "Cibernética y Sociedad", Weiner (1969) afirma que: sólo puede entenderse la sociedad mediante el estudio de los mensajes y de las facilidades de comunicación (…) en el futuro, desempeñarán un papel cada vez más preponderante (…) entre hombres y máquinas, máquinas y hombres y máquina y máquina" (p. 18). Y decide unir esa postura de ingeniería, con lo que los fisiólogos, como Walter Canon, habían desarrollado en las décadas anteriores bajo los títulos de "homeostasis" y estudios de comportamiento neuro-muscular.

Además hizo una analogía entre el comportamiento de los nuevos equipos digitales y el sistema nervioso humano, y este tipo de analogías biológicas – tecnológicas, se encargaría de desarrollar la teoría cibernética:

> El campo tiene un componente cuantitativo, heredado de control de la retroalimentación y la teoría de la información, pero es una herramienta cualitativa, analítica primaria; incluso se podría decir que una filosofía de la tecnología. La cibernética se caracteriza por una tendencia a universalizar el concepto de retroalimentación, viéndolo como el principio

> subyacente del mundo tecnológico. Algunas variantes estrechamente relacionadas incluyen: teoría de la información, ingeniería de factores humanos, la teoría de control, la teoría de sistemas. (Mindell, 2000).

Dentro de la cibernética como ciencia, la teoría del control y de la comunicación son aspectos fundamentales para el desarrollo de la cibernética. "En este contexto, el control se ha de entender principalmente como el control retroactivo, más precisamente como retroalimentación" (Vallée, 2009). Y en lo que respecta al centro de la teoría de la comunicación, al querer regular el comportamiento o el actuar, tanto de una máquina como de un ser o un grupo humano, la intención es hacerlo a través de un mensaje.

Wiener a su vez extrapola la Cibernética desde el gobierno de las máquinas y la regulación del actuar humano hasta el campo más extenso que es la sociedad. Al respecto señala que sólo se puede entender la sociedad mediante el estudio de los mensajes, a la vez que proyecta la complejidad social futura con la integración tecnológica al decir que en el futuro los mensajes desempeñarán un papel más importante entre hombres, máquina y hombre, máquina y máquina. (Castro & Filippi, 2010).

Según David Aurel (1966), hay cinco elementos que caracterizan la definición como ciencia y el desarrollo de la cibernética: 1) El pensamiento dominado; 2) el trabajo intelectual; 3) las ideas claras; 4) el pensamiento clarificable; y 5) el cálculo molecular. El pensamiento dominado, hace referencia al papel de los intermediarios, y como la cibernética se puede encargar de las labores, tanto de los ejecutantes como de quién trasmite el mensaje.

El trabajo intelectual es lo que se reconoce como el pensamiento humano, caracterizado por la continuidad, el movimiento dentro del movimiento, la perpetúa adaptación y la puesta al día de un plan de acción. Las ideas claras se refieren a todo pensamiento regulado comprensible o, por lo menos, normalmente reproducible, memorizable, comunicable y enseñable, a uno mismo y a los demás. En cuanto al pensamiento clarificable, es entregarle a una máquina, la capacidad de operar de una forma rigurosa y clara, lo que permita confiarle la toma de decisiones. El postulado, consiste en que toda reflexión puede ser mecanizada. El cálculo molecular se refiere a la capacidad de tomar cada elemento y movimiento, analizarlo y adaptarlo a las máquinas. (Aurel, 1966).

La cibernética se puede aplicar a una amplia gama de disciplinas, pero su origen y uno de sus campos más importantes desde su creación hasta el presente, es el sector militar:

> Para unificar la investigación civil y orientarla hacia las nuevas necesidades de la guerra, Roosevelt creó en junio de 1940 el National Defense Research Committe –NDRC- (…) Las investigaciones realizadas bajo los auspicios del NDRC se centraron en el desarrollo de la bomba atómica, el radar, la investigación operativa (desarrollo de modelos matemáticos y estadísticos para analizar y simular la toma de decisiones), y toda una serie de tecnologías subsidiarias. (De Gracia & Thomas, 2008, p. 262).

El sector más afectado y que necesitaba desarrollo con mayor urgencia era el aéreo. Aunque hubo un gran esfuerzo para su mejor, fue poco lo que se alcanzó, hasta la contratación de Norbert Wiener. Wiener atacó el problema de predecir las trayectorias de vuelo de aviones en una acción evasiva, reformulando el valor futuro de una función aleatoria, basado en su historia estadística. Esta generalización: "A partir de un problema específico entre hombre y máquina en cualquier aspecto del mundo que pueda ser expresado como datos de series de tiempo" (Mindell, 2000), Ser fundamentó la visión anticipada de las estrategias que definirían la cibernética.

Wiener (1965), respecto al perfeccionamiento de la artillería antiaérea, tuvo dos avances importantes. El primero, referido a la absoluta precisión que ha de llevar el proyectil para dar en el blanco, donde estableció que predecir el futuro de una curva, en este caso un aeroplano a gran velocidad, implica resolver una cierta operación sobre su pasado; el segundo alude al control humano de la máquina, es decir, los movimientos y características de la actuación del piloto, ya que este conocimiento es también determinante para solucionar el problema de que el proyectil alcance el blanco.

Junto al concepto de regenerador, Wiener también se refiere a otras dos ideas fundamentales que aparecen en sus investigaciones sobre ingeniería del avión, llevadas a cabo en colaboración con Julian H. Bigelow. La idea de mensaje y la de cantidad de información. Respecto a la primera, señala que:

> En la comunicación sobre ingeniería del avión se hizo claro que los problemas de ingeniería de control y de comunicación eran inseparables y que se centraban no sobre la técnica de ingeniería eléctrica sino sobre la noción más fundamental del mensaje, ya fuera transmitido por medios eléctricos y mecánicos o nerviosos, definiéndola como la secuencia continua o discontinua de sucesos medibles distribuidos en el tiempo. (Wiener, 1965).

La otra noción, cantidad de información, no solo es el capital en la teoría moderna de las comunicaciones, sino que su repercusión será enorme. El avance de la ingeniería de la comunicación supuso necesariamente el desarrollo de "una teoría estadística de la cantidad de información, en la que la cantidad y unidad de información era aquella transmitida como una sola decisión entre alternativas igualmente probables" (Wiener, 1965).

Como dice Wiener, y no ha cambiado con el paso del tiempo, la información es uno de los recursos más importantes para los Estados en la actualidad, es más; hoy en día, su importancia es aún mayor que antes. La teoría de la comunicación, se encarga de manejar la información y en la actualidad, siendo parte de la cibernética, se desarrolla en su mayoría en el ciberespacio. Las necesidades, en el caso de la cibernética, de carácter militar, dieron paso al desarrollo de herramientas para manejar la información: La creación de DARPA, "una organización desarrollada por el Pentágono para evitar la sorpresa tecnológica y profundizar en la investigación sobre ordenadores" (Singer & Friedman, 2014); y de igual manera, el surgimiento de ARPANET, una red de cuatro nodos, formándola a través de los Estados Unidos.

El ciberespacio es definido en la Estrategia Nacional para la Seguridad Del Ciberespacio en el 2003 como "El sistema nervioso, el sistema de control del país [...] compuesto por cientos de miles de ordenadores interconectados, servidores, routers, conmutadores y cables de fibra óptica que permiten trabajar a nuestras infraestructuras críticas" (Kuehl, 2009, p. 27). Por otro lado, el 8 de enero de 2008, La Casa Blanca en "La política para la ciber-seguridad", definió al ciberespacio como la red interdependiente de infraestructuras de tecnología de la información, que incluye el Internet, las redes de telecomunicaciones y sistemas informáticos, adheridos a procesadores y controladores en industrias críticas haciendo referencia a la participación del ciberespacio en las infraestructuras principales de los Estados.

En la actualidad, la mayoría de la información se encuentra en el ciberespacio. El objetivo principal es conseguirla y manejarla, y esta se ha convertido en la fuente de poder en la modernidad, esta mueve las decisiones políticas, económicas, militares, sociales e industriales. Los dirigentes y mandos necesitan información para obtener mayor precisión o ser más efectivos. Los sistemas de información se han convertido en el centro de gravedad de los países y esto los convierte en un objetivo crítico. El movimiento de la información de un sistema a otro a través de las redes de comunicación representa una vulnerabilidad explotable, lo que le convierte en un objetivo primordial para cualquier acción ofensiva (Miller, 1997).

Militarmente, el poder cibernético ha sido el instrumento más influyente de las últimas dos décadas. Tanto el poder cibernético y el ciberespacio han estado en el corazón de los nuevos conceptos y doctrinas de la guerra. Se ha convertido en un elemento indispensable de la capacidad militar basada en la tecnología moderna. Actualmente la búsqueda de información es un objetivo preponderante para los actores del Sistema Internacional. El espionaje cibernético presenta una forma menos costosa para los actores estatales, incluidas las empresas privadas, para la construcción de conceptos detallados de información sobre los competidores y adversarios. "Los espías cibernéticos pueden utilizar la información robada para cualquier número de propósitos, incluyendo la intimidación, la extorsión o el esfuerzo para prever o interrumpir las maniobras de la oposición política" (Lord, 2011).

La principal característica de la revolución cibernética es que los avances tecnológicos provocaron una gran base para la inteligencia militar en búsqueda de la información que "no sólo podría utilizarse para proporcionar una advertencia estratégica para la toma de decisiones, también podría estar directamente relacionada con las operaciones tácticas, y en ello permitieron el control completo del espacio de batalla" (Kaspersky, 2013). La información representa un recurso que se ve amenazado por "la creciente dependencia a los sistemas informáticos con acceso para almacenar, procesar y comunicar información digital crítica para los actores y el aumento de las comunicaciones a través de Internet" (Waterfall, 2011).

La sociedad moderna se basa en la disponibilidad y el acceso a la información, la cual está encargada de impulsar una economía próspera o una posición de poder. "En el mundo electrónicamente interconectado de hoy, la información se mueve a la velocidad de la luz, es intangible, y es de inmenso valor" (Schwartau, 1996). Dicho por Anne Wells Branscomb (1994), en casi todas las sociedades, el control y el acceso a la información se convirtieron en instrumentos de poder.

Al igual que la diplomacia, la competencia económica, o el uso de la fuerza militar, la información en sí misma es un aspecto clave del poder nacional y, más importante aún, se está convirtiendo en un recurso estatal cada vez más vital que apoya la diplomacia, la competencia económica y el empleo eficaz de las Fuerzas Militares.

La cibernética es un campo con una gran influencia en el aspecto militar, y los conflictos, con estos importantes avances, se han adaptado a las nuevas exigencias del ciberespacio y la guerra ha mutado y posee nuevas características. En la actualidad hay cuatro escenarios en los cuales se desarrolla la guerra, relacionados con la cibernética: 1) Information Warfare; 2) los efectos de las armas cibernéticas en los centros de gravedad estatales; 3) el desarrollo tecnológico de armamento; y 4) la tecnología cyborg.

"El uso de la información en la guerra no es nada nuevo" (Jones, Kovacich & Luzwick, 2002). Los que tenían la mejor información de la manera más rápida, y eran capaces de actuar sobre ella lo más pronto posible, eran por lo general los vencedores en la batalla. La nueva tendencia de guerra en la cual la información se maneja en el ciberespacio y se usa como arma, es la guerra de la información.

> El nombre para todos los conflictos futuros, así como para asegurar un lugar como un actor clave en la escena política internacional del nuevo milenio será el dominio de la información. Los Estados y los ejércitos que reinarán totalmente sobre los campos de batalla militares y políticos del mañana sólo serán aquellos capaces de dominar el flujo de información y al mismo tiempo evitar que sus potenciales adversarios hagan lo mismo. (Delibasis, 2007).

La planificación militar se desplaza de la exclusividad terrestre, marítima o aérea, hacia la opinión de que el poder de combate se puede mejorar a través de redes y tecnologías que controlan el acceso y manipulan directamente la información de comunicaciones. "Como resultado, la información en sí es tanto una herramienta como un objetivo de la guerra" (Wilson, 2004).

Para Schwartau (1996) el mundo es un espacio donde el poder de usurpar el conocimiento y la información, da fuerza al poder militar. Totalmente dependiente de las nuevas herramientas de alta tecnología que hacen que la información esté disponible instantáneamente para cualquier persona, en cualquier lugar, en cualquier momento. Generando un conflicto donde la información es el premio, el botín de guerra, donde los ordenadores se convierten en las armas ofensivas de gran eficacia y que define los equipos y sistemas de comunicación como objetivos primarios obligados a defenderse contra balas y bombas invisibles.

La Guerra de la información es capaz de permitir precisión y profundidad en los ataques de los Estados, por lo tanto, alteró dramática y permanentemente los medios potenciales de cualquier beligerante para hacer la guerra. En los últimos años, el concepto de guerra de información se ha vuelto popular en ciertos círculos de las autoridades de defensa. "El concepto tiene sus raíces en el hecho indiscutible de que las tecnologías de la informa-

ción y la información son cada vez más importantes para la seguridad nacional en general y específicamente a la guerra" (Libicki, 1995).

Según la definición de la Fuerza Aérea de los Estados Unidos, la Guerra de Información comprende "cualquier acción de negar, explotar, corromper o destruir la información del enemigo y sus funciones; a la vez de proteger nuestras propias funciones de información militar contra esas acciones y la explotación" (Nichiporuk, 1999). Existen dos rasgos principales de la Guerra de Información: "El primero es que es una forma directa de ataque y el segundo es que no implica en modo alguno la intervención de las funciones perceptivas y analíticas de un adversario potencia" (Delibasis, 2007).

La guerra de información implica una serie de medidas o "acciones destinadas a proteger, explotar, corromper, negar o destruir información o recursos de información con el fin de lograr una ventaja significativa, objetiva, o la victoria sobre un adversario" (Crawford & Cronin, 1999). Un objetivo típico de la guerra convencional es destruir o degradar los recursos físicos del enemigo, mientras que el objetivo de la Guerra de Información es apuntar a los activos y la infraestructura de la información, de tal manera que el daño resultante pueda no ser inmediatamente visible o detectable, pero tenga un efecto devastador en alguna medida, a corto, mediano o largo plazo; según el interés del atacante.

Para Maria Rosaria Taddeo (2012) la definición general de Guerra de la información es el uso de las TIC con fines, tanto ofensivos o defensivos para entrometerse, interrumpir, o controlar los recursos del oponente. Y agrega que debe ser aprobada por un Estado y destinado a la inmediata alteración o control de los recursos del enemigo y se libra dentro del medio ambiente informativo, con agentes y objetivos que van tanto en los dominios físicos y no físicos.

La guerra de información es la forma en que los militares han tradicionalmente descrito "las operaciones que tratan de entrar en la mente e influenciar la toma de decisiones del enemigo" (Anderson, 2010). Con la cibernética, la idea es utilizar las modernas tecnologías de la información para los mismos fines. Los objetivos pueden ser altamente estratégicos, tales como enviar directrices falsas a los principales líderes, a inserciones más tácticas, poniendo en peligro los sistemas de armas individuales y sus sensores.

A pesar de sus inmensas diferencias, al igual que en la guerra clásica, los objetivos materiales de las operaciones de guerra informática se adecúan al nivel de planeamiento y ejecución:

> En el nivel táctico serán los centros de comunicaciones, comando y control enemigos, de logística o aquellos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la conducción de las operaciones militares. En el nivel operacional, podrán llegar a ser las líneas de comunicación, logísticas, de comando y control operacional del adversario, centros de desarrollo de tecnología, así como capacidades y actividades relacionadas. Por último, en el nivel estratégico, se podrán incluir objetivos nacionales, influyendo en todos los ámbitos (políticos, militares, económicos o relacionados con la información). (López, 2007).

Clay Wilson (2004) y Fred Schreier (2012), apoyados en la teoría del Departamento de Defensa de los Estados Unidos, hablan de las Operaciones de Información como los medios para llevar a cabo la Guerra de la Información. Las clasifican por cinco capacidades básicas: Operaciones psicológicas, engaño militar, de seguridad operacional, operaciones de red informática, y la guerra electrónica. Estas capacidades están destinadas a influir en los tomadores de decisiones extranjeros y proteger la toma de decisiones internas, y para afectar o defender los sistemas de información, y la información que soporta los tomadores de decisiones, sistemas de armas, mando y control, y las respuestas automáticas.

El engaño militar orienta a un enemigo a cometer errores al presentar información, imágenes o declaraciones falsas (Departamento de Defensa, 2010). Las Operaciones de Seguridad se definen como procesos de identificación de la información que es fundamental para las operaciones de amistad y que podrían permitir a los adversarios atacar las vulnerabilidades operacionales (Departamento de Defensa, 2010). Las Operaciones de Redes

Informáticas incluyen la capacidad para atacar y desbaratar las redes de computadoras, la defensa de los propios sistemas de información y comunicaciones, y explotar las redes de ordenadores enemigo a través de la recolección de inteligencia, por lo general hecho a través del uso de código de computadora y las aplicaciones informáticas (Chesney, 2013).

La Guerra Electrónica se define como cualquier acción militar que implica la dirección o el control de la energía del espectro electromagnético para engañar o atacar al enemigo (Departamento de Defensa, 2007). Por último, las operaciones psicológicas se planifican para transmitir información seleccionada al público extranjero dirigida a influir en sus emociones, motivos, razonamiento objetivo, y en última instancia el comportamiento de gobiernos, organizaciones, grupos e individuos extranjeros (Axelband, 2013).

La guerra informática constituye, hoy en día, una parte del conflicto armado que se encuentra en pleno desarrollo. Las investigaciones actuales, en el plano de la Defensa, apuntan a transformar tecnologías de informática en capacidades bélicas críticas en campos tales como señales, imágenes, inteligencia, fusión y gestión de información, computación avanzada, operaciones cibernéticas y Comando y Control.

El siguiente escenario donde la cibernética y la guerra se plantean juntas es el daño o ataque a los centros de gravedad estatal, a través de herramientas cibernéticas. Generalmente los elementos especialmente sensibles de un Estado son sus centros de gravedad, "que abarcan los sectores y la sociedad pública y privada en general. Esto va más allá de la infraestructura física, para incluir datos, que pueden considerarse una forma de infraestructura lógica o infraestructuras críticas de información" (Clemente, 2013).

La mayoría de las definiciones de centros de gravedad estatal, como aquellos "sistemas que son de vital importancia para la sociedad" (Kelly, Peerenboom & Rinaldi, 2001). Algunos criterios que pueden ser tomados en cuenta para reconocer un centro de gravedad estatal pueden ser:

> Las posibles víctimas si ocurre una falla, en términos del número de víctimas mortales o heridos; los posibles efectos económicos, en términos de pérdidas económicas, el deterioro de los productos o servicios y efectos o daños ambientales o los posibles efectos sobre la población, en términos de pérdida de la confianza del público, el sufrimiento físico y la alteración de la vida cotidiana, incluyendo la pérdida de servicios esenciales. (Angelini, Arcuri, Baldoni, & Ciccotelli, 2013).

Para autores como Angelini, Arcuri, Baldoni, & Ciccotelli (2013), los centros de gravedad estatal son todas las redes y sistemas, incluyendo las instalaciones de la industria, las instituciones, y su distribución, que operan en sinergia y producen un flujo continuo de bienes y servicios esenciales para la organización, la funcionalidad y la estabilidad económica de un país industrializado moderno, cuya destrucción o indisponibilidad temporal puede causar un impacto debilitante en la economía, la vida cotidiana o la capacidad de un país para defenderse.

Los centros de gravedad de los Estados, sistemas fundamentales para la estructura organizativa y los mecanismos de funcionamiento de las instituciones empresariales, industriales y gubernamentales; están ampliamente amenazados en la actualidad, por la interdependencia que existe entre ellos. Los tipos de interdependencia entre las infraestructuras se volvieron más importantes, por el aumento de la exposición al ciber-riesgo del sector privado y el sector público en un contexto nacional e internacional. La importancia de riesgo cibernético es debido a sus efectos desastrosos potenciales:

> Hay una creciente conciencia de la vulnerabilidad de la infraestructura crítica de la nación a los ataques de red. Transporte, la banca, las telecomunicaciones y la energía son algunos de los sistemas más vulnerables y pueden estar sujetos a los siguientes modos de ataque: Las amenazas internas o el acceso anónimo a las redes protegidas a través de Internet y Control de Supervisión y Adquisición de Datos –SCADA-. (Carr, 2010).

La naturaleza de las amenaza es tan amplia que cualquier aspecto del mundo que dependa del dominio cibernético está potencialmente en riesgo (OTAN, 2010). Por lo tanto, el motivo de preo-

cupación son las acciones adversas que ponen en peligro la integridad y la seguridad de los centros de gravedad nacionales; desestabilizar el sistema financiero; permitir el acceso a información clasificada de importancia nacional como los secretos comerciales, comercialmente explotables; o socavar de alguna otra manera significativa la capacidad de confiar en los sistemas de información y tecnología de las comunicaciones -TIC- para objetivos de seguridad nacionales pertinentes:

> Los Estados son cada vez más vulnerables a los ataques cibernéticos, estos podrían tener efectos catastróficos sobre los centros de gravedad, así como ser capaces de dañar severamente las economías nacionales. Los ataques cibernéticos masivos incluso en sólo un segmento del sistema son difíciles de controlar, y sus consecuencias podrían ser incalculables. Ellos podrían alterar decisivamente las ecuaciones de poder, la estabilidad de todo el entorno digital del que la sociedad depende, mucho más allá de solo afectar las partes que participan en un conflicto. (Schreier, 2012).

Aquellos encargados de tomar decisiones, principalmente en el sector militar, deben enfrentar amenazas a su trabajo a través de ciber-ataques, y deben, en primer lugar, asumir que los centros de gravedad pueden ser atacados y se deben tomar medidas para protegerlos, es decir, endurecer la infraestructura o mejorar sus defensas activas. El presupuesto para el endurecimiento o la defensa activa siempre será limitado. Así que, por lo general, el analista se encargará de crear una lista priorizada de "activos defendidos", es decir, aquellos más necesitados de protección, junto con una lista de posibles medidas defensivas, y entregar dichas listas a los tomadores de decisiones de alto nivel (Brown, Carlyle, Salmerón, & Wood, 2005).

Los ataques cibernéticos se han presentado hacia las estructuras más importantes de los Estados, y aunque es claro, que como característica del ciberespacio, el anonimato impide adjudicarlos a un actor específico, si se puede retratar que ha sucedido en casos como Estonia y Georgia. En el caso estonio, el país se basa en la Internet para su infraestructura crítica: "Redes electrónicas son esenciales para el funcionamiento de las operaciones gubernamentales, redes de energía eléctrica, servicios bancarios, e incluso el suministro de agua de Tallin. En Estonia, el 97% de las transacciones bancarias se producen en línea" (Herzog, 2011). Durante un período de dos semanas en abril y mayo de 2007 Estonia fue víctima de un ataque cibernético masivo sufrido en su infraestructura de información.

> Al mismo tiempo que se desarrollaban disturbios civiles, el gobierno de Estonia y los medios de comunicación nacionales estonios fueron hackeados con afectación significativa. Algunos de los ataques al sistema eran vandalismo sobre sitios web y algunos fueron ataques de denegación de servicio. Los ataques comenzaron poco a poco hasta un gran ataque que culminó en la caída del sistema de Internet de Estonia el 9 de mayo de 2007. (Landler & Markoff, 2009).

Por otro lado, en el caso de Georgia, la guerra que comenzó oficialmente el 7 de agosto de 2008 de manera física, aparentemente con anterioridad había iniciado de manera cibernética. Al parecer "54 sitios web en Georgia relacionados con las comunicaciones, las finanzas y el gobierno fueron atacados por elementos corruptos" (Hollis, 2011). Así como tanques y tropas estaban cruzando la frontera y bombarderos volaban, los ciudadanos georgianos no podían acceder a los sitios web para obtener información e instrucciones. Las autoridades de Georgia descubrieron su acceso a Internet y las redes de comunicación eran excepcionalmente vulnerables.

Los centros de gravedad estatales son objetivos normales para los planificadores militares con la misión de obtener una ventaja estratégica. Los ataques cibernéticos potencialmente podrían producir trastornos, y posiblemente a menor costo para el atacante que cualquier otro mecanismo que se pueda usar. La capacidad de interferir con las comunicaciones y logística por ventaja operativa o táctica es amplia usando ciber-ataques. (Schreier, 2012). Por lo tanto, para una serie de escenarios de conflicto, un oponente podría pensar de manera razonable y usar ataques cibernéticos a interferir con los esfuerzos para avanzar, desplegar, y suministrar fuerzas, y ser capaz de desestabilizar por completo

un estado únicamente mediante las redes que unen sus centros de gravedad.

En tercer lugar, como escenario de aplicación de la cibernética en la guerra se encuentra el desarrollo tecnológico en armamentos, como drones y el avance en la robótica; lo que ha permitido el mejoramiento del rendimiento de las Fuerzas Militares, aprovechando la rápida evolución de la tecnología. Las tecnologías emergentes se pueden utilizar para gran cantidad de propósitos, varios de los cuales están relacionados con el conflicto entre Estados. De este modo, se argumenta que "las tres tecnologías emergentes más prominentes tienen efectos mixtos sobre la conducción de la guerra: Los avances en el uso de aviones no tripulados, sistemas espaciales y capacidades cibernéticas" (Grauer, 2013). Pueden ser muy beneficiosos en el mejoramiento de la calidad de batalla y protegiendo la vida de quienes se enfrenta, pero a su vez son muy costosos e igualmente pueden ser muy vulnerables, como todas las tecnologías cibernéticas.

El armamento no tripulado y la robótica, son herramientas cinéticas y cibernéticas sofisticadas de guerra, y mejoran las capacidades de los actores para usar la fuerza directa e indirecta. Las nuevas armas de ataque en fase de desarrollo que emplean enjambres de aviones no tripulados en miniatura son más sofisticadas, y las nuevas mejoras en la robótica, en teoría podrían, obviar la necesidad de la presencia humana en el campo de batalla durante un ataque:

> Ofensivamente, cámaras y pistolas de montaje en vehículos a control remoto guiadas por el mando directo de los *Sistemas de Armas Especiales* para la *Observación* –SWORDS- o plataformas aéreas como el avión no tripulado *Predator* permite a los militares impulsar el poder de fuego en áreas y situaciones en las que podría ser demasiado peligroso enviar una persona. (Coeckelbergh, 2013).

Este nuevo tipo de armas, aviones no tripulados y sistemas robóticos, pueden utilizarse para proteger perímetros. Los drones de vigilancia pueden patrullar las fronteras para vigilar los cruces ilegales. Igualmente, la mejora de las capacidades sensoriales eventualmente permitirá que los sistemas automatizados reaccionen y destruyan las amenazas entrantes más rápidamente que sus contrapartes tripuladas. Las futuras versiones de estos sistemas sólo aumentará la cantidad de fuerza directa de que los actores tecnológicamente capaces puedan ejercer en los próximos conflictos. (Grauer, 2013).

Los drones son extremadamente útiles para los militares porque permanecen en el aire durante mucho tiempo: pueden volar de 24 a 36 horas, que es mucho más de lo que los pilotos en un avión podrían volar. Los militares pueden estudiar de forma continua, por ejemplo, la ubicación de presuntos militantes o terroristas para muchas horas:

> Los sistemas no tripulados ya han reformado profundamente la estrategia de defensa y prioridades de adquisiciones estadounidenses y son cada vez más importante en las fuerzas armadas de todo el mundo. Miles de sistemas no tripulados de varios tipos se encuentran ahora en el inventario de Estados Unidos. Al menos 75 países están invirtiendo en sistemas no tripulados. (Brimley y Work, 2014).

Por otro lado, la robótica militar es un campo importante en la tecnología militar, el cual se basa en el uso de computadores. Los conflictos armados futuros se caracterizan por el aumento del uso y la confianza en robots militares. Una de las características distintivas de aquellos robots que puedan participar en la guerra "es que, a diferencia de anteriores conflictos, se lucha con armas no tripuladas o deshabitadas" (Giacca & Leveringhaus, 2014). Contrario a un tanque, donde hay un grupo de soldados en el interior, no hay soldados en el interior del robot. Es más, en la gran mayoría de los casos, los soldados que manejan la tecnología pueden estar a miles de kilómetros del campo de batalla.

Las armas robóticas tienen dos formas de funcionar. Primero, un operador humano controla el proceso de orientación a través de control remoto. O, una vez que el operador humano ha programado el robot con su misión, el robot puede llevar a cabo los pasos del proceso de focalización sin que exista más intervención por parte de un operador humano (Giacca & Leveringhaus, 2014). Durante los últimos 20 años, los vehículos robóticos milita-

res se han construido utilizando todos los modos de locomoción y hacen uso de los nuevos paradigmas de software. "En los robots militares se encuentran las principales aplicaciones de vigilancia, reconocimiento, localización y destrucción de minas y artefactos explosivos improvisados, así como para la ofensa o ataque" (Mies, 2010).

Respecto al software que maneja los robots, puede ir desde el nivel más bajo, que es básicamente reflexivo, y permite al robot reaccionar casi instantáneamente a una entrada sensorial particular; pasando por la función reactiva, que presta servicios de supervisión y traduce comandos de ejecución; hasta llegar al nivel más alto que incluye Inteligencia Artificial tal como la planificación y el aprendizaje, así como la interacción con los seres humanos, la localización y navegación. (Abney, Bekey & Lin, 2008).

Un robot, sobre todo en un contexto militar, es una máquina motorizada que "detecta, piensa (en una deliberación, el sentido no mecánico), y actúa" (Abney, Bekey & Lin, 2008). Los robots pueden operar de manera semi o totalmente autónoma, pero no pueden depender enteramente de control humano. Los robots pueden ser prescindibles o recuperables, y pueden llevar una carga letal o no letal. Y los robots pueden ser considerados como agentes, es decir, tienen la capacidad de actuar en un mundo, y algunos incluso pueden ser agentes morales. Los robots, en un futuro, serían lo suficientemente "inteligentes" como para tomar decisiones que por ahora solo pueden tomar los humanos, ampliarían el espacio de batalla por alcanzar grandes áreas de terreno y representan un importante multiplicador de fuerza.

Los robots podrían traer beneficios significativos en el campo de la guerra. Reemplazarían a los humanos en trabajos tediosos o peligrosos, también pueden llegar a ser más exigentes, eficientes y eficaces. "Su enfoque desapasionado y distante a su trabajo podría reducir significativamente los casos de conducta no ética en tiempos de guerra" (Yakovleff, 2014). Por otro lado, aunque las atrocidades en tiempos de guerra se han producido desde el comienzo de la historia humana, pueden reducirse en la medida en que los robots participen en el campo de batalla, generando una reducción en las pérdidas de vida humana y en los comportamientos crueles.

> En el sector de la robótica, además de existir razones para profundizar en su investigación, todavía hay enormes desafíos por resolver, tales como la dificultad fundamental de la programación de un robot para distinguir confiablemente combatientes enemigos de los no combatientes, como lo exigen las leyes de la guerra y la mayoría de normas de intervención. (Abney, Bekey & Lin, 2008, p. 90).

Un régimen de guerra basado en los sistemas no tripulados y autónomos y la tecnología robótica, tiene el potencial de cambiar los conceptos fundamentales básicos de la estrategia de defensa, incluyendo la disuasión, la tranquilidad y la compulsión. Estos sistemas tendrán características diferentes que sus contrapartes tripuladas y reconfigurarán las posiciones militares y el comportamiento de las Fuerzas Militares de todo el mundo, además de la forma de tomar decisiones sobre el uso de la fuerza (Brimley & Work, 2014).

En último lugar, la tecnología *Cyborg,* la cual asume la definición más básica de la cibernética: El control y la comunicación sobre una máquina. El vocablo nace de la unión entre *cybernetic* y *organism,* para dar la noción del cuerpo como máquina, es decir, la mecanización de las funciones del ser humano. Una definición aplicable en este contexto es "un ser humano corregido en sus defectos y carencias, y a la vez potenciado en sus facultades, mediante el empleo y la implantación de tecnologías protésicas en su organismo" (Koval, 2006).

El término fue acuñado en 1960 por los doctores Manfred Clynes y Nathan Kline, para referirse un ser humano "mejorado" que soportara las duras condiciones de la atmósfera extraterrestre. "Para el organismo complejo y funcionando inconscientemente como un sistema homeostático integrado, proponemos el término *Cyborg"* (Clynes & Kline 1995, pp. 30-31). La idea surgió de un proyecto para la Fuerza Aérea de EE.UU. en el que se buscaba potenciar los órganos vitales del hombre y alterar sus constantes psicofísicas para robustecer al organismo en condiciones precarias.

> Las preocupaciones giraban en torno a algunos problemas básicos que requerían prontas soluciones: estado de alerta y vigilia, efecto de radiación, problemas metabólicos y controles térmicos, oxigenación y reducción del carbono, entrada y salida de fluidos, control cardiovascular, mantenimiento muscular, problemas de percepción, variación de la temperatura y de la presión externas, trastornos psiquiátricos, etc. Pocos años después, el concepto de *cyborg* excedería al campo militar para filtrarse en el mundo civil. Lo mismo que Internet, un proyecto de tecnología militar acabaría por ser difundido, expandido y modificado en mil formas en su utilización civil. (Koval, 2006, p. 11).

La implicación en la guerra actualmente de la relación entre tecnología y cuerpo humano es muy importante. Nuevos tiempos parecen requerir nuevos soldados para el "trabajo" de defender la nación. Los discursos militares han construido el soldado cyborg. "El cuerpo humano sigue siendo un sitio clave de injerto tecnológica, es el sitio de estas modificaciones, si se trata del *wetware* (la mente y las hormonas), el *software* (hábitos, habilidades, disciplinas), o el *hardware* (el cuerpo físico)" (Masters, 2005).

Actualmente, el desarrollo de tecnologías que permitan el uso del término "cyborgs", es muy conocido a nivel mundial. En los últimos 10 años, el desarrollo de este tipo de tecnología ha estado entre los principales intereses en el entorno internacional. Los avances tecnológicos han obligado a los ingenieros a buscar formas para aplicar tecnología, tanto en animales como en seres humanos.

Los ingenieros, angustiados por la miniaturización de los circuitos de computadora y técnicas de micro-fabricación, han hecho todo lo posible para construir máquinas voladoras pequeñas que imiten la capacidad locomotora de los insectos, lo que les permitiría avances significativos en tareas donde entre más pequeño sea el objeto, mucho mejor:

> El *DelFly Micro,* presentado en 2008, por investigadores de la Universidad Tecnológica de Delft en los Países Bajos, pesa sólo tres gramos, tiene una envergadura de 100 milímetros y puede llevar una pequeña cámara de video. El que se produjo en el Laboratorio Microrobótico de Harvard es aún más pequeño, aunque una vez puesto en marcha, no se puede controlar. El talón de Aquiles de estos insectos mecánicos, sin embargo, es la cantidad de energía que consumen: nadie ha descubierto la manera de empacar suficiente energía en baterías en miniatura para abastecerlos por más de unos pocos minutos de vuelo. (Maharbiz, & Sato, 2010).

Este tipo de "Insectos Cyborg" podrían potencialmente tener muchos usos militares, incluyendo la capacidad de saber cuántas personas hay en el interior de un edificio o de una cueva y determinar quiénes son antes de decidir si se deben enviar tropas de soldados a enfrentar la amenaza.

El éxito inicial de las técnicas (Chips en insectos y tiburones) se ha traducido en un aumento de la investigación y la creación de un programa llamado Hybrid Insect Micro-Electro-Mechanical System, -HIMEMS-. Su objetivo, según la Oficina de Tecnología de la DARPA, es "el desarrollo de interfaces hombre-máquina con insectos, fuertemente acoplados mediante la colocación de sistemas micro-mecánicos dentro de los insectos durante las primeras etapas de la metamorfosis" (Naveen & Nagoor, 2014).

Igual que el desarrollo de la tecnología sobre animales; aún más importante es el desarrollo humano. El ejército estadounidense está invirtiendo millones de dólares en proyectos como *Ekso Bionics Human Universal Load Carrier* –HULC-, un "exoesqueleto portátil, al estilo de Iron Man, que da a los soldados una fuerza sobrehumana" (House, 2014). Su avanzada Asociación de Proyectos de Investigación de Defensa –DARPA-, trabaja a su vez en robots asesinos de pensamiento controlado, cascos de pensamiento para permitir la comunicación telepática y las interfaces cerebro-ordenador –BCI- para dar a los soldados sentidos adicionales, como la visión nocturna y la capacidad de ver los campos magnéticos causados por las minas terrestres.

> El objetivo del exo-esqueleto es crear un objeto con bajo consumo de energía (menos de 100 vatios), ligero (40 libras), debajo de la ropa, que permita a los soldados que van a pie, correr o subir más lejos y más rápido

> sin esfuerzo adicional (…) El Guerrero Web –EKSO- es controlado por un ordenador conectado a la mochila de camuflaje. (Upbin, 2014).

En este momento, DARPA, la Agencia de Proyectos de Investigación Avanzada de Defensa, está buscando el desarrollo de una nueva generación de tecnologías que unan los sistemas biológicos y electrónicos. Una nueva división de la investigación y desarrollo militar será experimentar con tecnologías de la fusión de la vida con las máquinas. El proceso de desarrollo de esta tecnología se realizará desde la Oficina de Tecnologías Biológicas -BTO-, la cual utilizará los organismos biológicos como la base de nuevos mecanismos de defensa. La investigación en estos campos ya ha sido promovida por las oficinas de Ciencias de la Defensa -DSO- y *Microsystems Technology* -MTO-:

> La Oficina de Tecnologías Biológicas se centrará en ayudar a los que han perdido extremidades, además de una amplia variedad de otros proyectos de fusión de los seres humanos y las máquinas. Hand Propiocepción y Touch Interfaces -HAPTIX- es una de las primeras tecnologías que serán exploradas por el grupo. Este proyecto tiene el objetivo de crear prótesis que proporcionarán la sensación del tacto a los usuarios (…) La tecnología desarrollada por el BTO podría ser utilizado para ayudar a los soldados que se recuperan de lesiones incapacitantes. También podría ser utilizado para permitir la construcción de super-soldados, con poderes mucho más allá de las capacidades humanas. (Maynard, 2015).

La BTO se encargará de estudiar los sistemas del ser humano, que le permitan agilizarlos y potencializarlos, además de buscar materiales que sean más eficaces, ligeros y resistentes para la creación de las tecnologías y se asimilen más a aquellos que componen el cuerpo humano; y pretende crear aparatos de diagnóstico y software para dar a los tomadores de decisiones un diagnóstico rápido y específico de la infección, para entender la propagación de la enfermedad; entre otros objetivos que se pretenden cumplir con la creación de este departamento. (Tucker, 2014).

Desde su conceptualización, la cibernética ha tenido un impacto significativo sobre una amplia variedad de disciplinas en todo el mundo, si bien como disciplina en particular aún no se encuentra definida de manera universal. Aun así, ha tenido gran influencia en numerosas ciencias, incluyendo algunas de las más prominente, es más; es uno de los pilares en el discurso y la visión del mundo hoy, profundamente arraigado a la cultura tecnológica.

Los mayores avances, en ataques cibernéticos por las redes, robots sofisticados, aparatos no tripulados, o mecanismos cyborg, constituyen el último episodio escrito de la imparable carrera en la cual los hombres se han trazado como meta simplificar hasta el máximo, el esfuerzo que realizan para conocer, controlar y dominar la naturaleza.

El sector militar ha ofrecido y recibido beneficios muy importantes respecto a la disciplina cibernética. Esto se debe a que la gran mayoría de creaciones con respecto a avances cibernéticos ha surgido en las Fuerzas Militares, en la búsqueda de mejores tácticas y técnicas de defensa y ataque. La creación del término cibernética, del incipiente Internet, de la operación de información, de los drones, la robótica o la tecnología cyborg, han sido establecidos por hombres militares.

El desarrollo de la guerra ha obligado a los actores a adaptarse a los nuevos escenarios; y en una sociedad tan interdependiente, el escenario cibernético ha cobrado una relevancia que nunca antes se había reconocido. Las interconexiones entre todos los sistemas estatales, y en general todos los actores del Sistema Internacional, los hace más vulnerables a los ataques cibernéticos que pueden llegar a ser un factor desestabilizante muy importante. Por lo tanto, las nuevas amenazas en los nuevos escenarios exigen respuestas innovadoras y avances tecnológicos que no choquen con los nuevos entornos, y se adapten a ellos.

Referencias

Abney, K., Bekey, G., & Lin, P. (2008). Autonomous Military Robotics: Risk, Ethics, and Design. California: Department of the Navy, p. 112.

Anderson, R. (2010) Security Engineering: A Guide to Building Dependable Distributed Systems. 2 ed. New Jersey: John Wiley & Sons, p. 1080.

Angelini, M.; Arcuri, M. C.; Baldoni, R. & Ciccotelli, C. (2013) Critical Infrastructure and Other Sensitive Sectors Readiness. Roma, p. 90.

Ashby, W. (1997). Introducción a la cibernética. Buenos Aires: Nueva Visión.

Aurel, D. (1966) La cybernétique et l'humain. París: Gallimard.

Axelband, E. (2013) Redefining Information Warfare Boundaries for an Army in a Wireless World. RAND Corporation.

Branscomb, A. W. (1994) Who owns information?: From privacy to public access. New York: Basic Books, p. 241.

Brimley, S. & Work, R. (2014). 20YY: Preparing for War in the Robotic Age. Washington DC: Center for a New American Security, p. 44.

Brown, G; Carlyle, M; Salmerón, J. & Wood. (2005). Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses. *Tutorials in Operations Research*, pp. 102 – 123.

Carr, J. (2010). *Inside Cyber Warfare*. California: Mike Loukides.

Castaño Ales, E. (2000). Los orígenes del arte cibernético en España. El seminario de Generación Automática de Formas Plásticas del Centro de Cálculo de la Universidad de Madrid (1968-1973). Alicante: Madrid.

Castro, C. & Filippi, L. (2010). Modelos Matemáticos de Información y Comunicación, Cibernética (Wiener, Shannon y Weaver): Mejorar La Comunicación es el Desafío de Nuestro Destino Cultural. Periodismo, Comunicación y Sociedad. 3(6) pp. 145 – 161.

Chesney, R. (2013). Computer Network Operations and U.S. Domestic Law: An Overview. En: International Law Studies, p. 89.

Clemente, D. (2013). Cyber Security and Global Interdependence: What Is Critical? Londres: CHATMAN HOUSE, p. 46.

Clynes, M. E. & Nathan, S. K. (1995). Cyborgs in Space. Hables Gray, Figueroa-Sarriera y Mentor (eds.) *The Cyborg Handbook*. Nueva York: Routledge.

Coeckelbergh, M. (2013). Drones, Information Technology, and Distance: Mapping the moral epistemology of remote fighting. En: Ethics and Information Technology. 15, pp. 87 – 98.

Crawford, H & Cronin, B. (1999). Information Warfare: It Application in Military and Civilian Contexts. En: *The Information Society, 15*, 257 – 263.

De Gracia, M. & Thomas, M. (2008). El origen del movimiento cibernético: Las conferencias Macy y los primeros modelos mentales. En: *Revista de Historia de la Psicología. 29 (314)* pp. 261 – 268.

Delibasis, D. (2007). The Right to National Self-defense: In Information Warfare Operations. Tennessee: Arena.

Departamento de Defensa de los Estados Unidos. (2007). Electronic Warfare. Recuperado de: http://fas.org/irp/doddir/dod/jp3-13-1.pdf

Departamento de Defensa de los Estados Unidos. (2010). Dictionary of Military and Associated Terms. Washington D.C. Recuperado de: http://fas.org/irp/doddir/dod/jp1_02.pdf

Departamento de Defensa de los Estados Unidos. (2010). Joint Security Operations in Theater. Recuperado de: http://www.dtic.mil/doctrine/new_pubs/jp3_10.pdf

Friedman, A. y Singer, P. W. (2014). Cybersecurity and Cyberwar: What everyone needs to know. New York: Oxford University, p. 320.

Giacca, y Leveringhaus, A. (2014). Robo-Wars: The Regulation of Robotic Weapons. Oxford: Oxford Martin School, p. 32.

Grauer, R. (2013). Old Wine in New Bottles: The Nature of Conflict in the 21st Century. *The Whitehead Journal of Diplomacy and International Relations*. Febrero. pp. 9 – 23.

Herzog, Stephen. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational

Responses. *Journal of Strategic Security*. Junio. 4(2) pp. 49 – 60.

Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. *Small Wars Journal,* Enero 6(1), p. 10.

House, A. (2014. Octubre, 20). The Real Cyborgs. *The Telegraph.* Recuperado de: http://s.telegraph.co.uk/graphics/projects/the-future-is-android/

Jones, A.; Kovacich, G. & Luzwick, P. (2002). Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages. Florida: Auerbach Publications, p. 664.

Kaspersky, E. (2013). Who's spying on you? Moscu: Kaspersky Lab, p. 33.

Kelly, T. K., Peerenboom, J. P. y Rinaldi, S. M. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* pp. 11-25.

Koval, S. (2006). Androides y Posthumanos: La integración hombre-máquina. Recuperado de: http://www.diegolevis.com.ar/secciones/Articulos/santiago_koval1.pdf

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. *Cyberpower and National Security.* 1 ed. Virginia: Franklin D. Kramer, Larry Wentz, Stuart H. Starr.

Landler, M. y Markoff, J. (2009. Mayo, 27) Digital Fears Emerge After Data Siege in Estonia. *The New York Times*. Recuperado de: http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0

Libicki, M. (1995) What is Information Warfare? Washington D.C: ACT, p, 104.

López, C. C. (2007). La Guerra Informática. *Boletín del Centro Naval.* Mayo-Agosto. N. 817. pp. 219 – 224.

Lord, K. & Sharp, T. (2011). America's Cyber Future. Security and Prosperity in the Information Age. Washington, D.C. Center of New American Security. Volume I.

Maharbiz, M. y Sato, H. (2010). Cyborg Beetles. Scientific American.

Masters, C. (2005). CYBORG SOLDIERS AND MILITARIZED MASCULINITIES. *International Feminist Journal of Politics. 7(1),* pp. 112 – 132.

Maynard, J. (2015. Abril, 3). DARPA heads for robot-human hybrid: Are cyborgs on the way *Tech Times.* Recuperado de: http://www.techtimes.com/articles/5137/20140403/darpa-robot-human-hybrid-cyborgs.htm

Mies, G. (2010). Robotics 2010 development of robotics and automation in industry. *Debreceni Műszaki Közlemények*, Octubre, pp. 57 – 68.

Miller, J. (1997). Information Warfare: Issues and Perspectives. En: Sun Tzu and Information Warfare. Robert Neison: Washington, D.C. pp. 145 – 167.

Mindell, D. A. (2000). Cybernetics: Knowledge domains in Engineering systems. Research paper, Massachusetts Institute of Technology.

Naveen, S. & Nagoor, M. (2014). Cyborg technology. Krishnasamy College of Engineering and Technology. Recuperado de: http://www.ifet.ac.in/pages/extsymp14/exsymp14/papers/MCA/MCA014.pdf

Nichiporuk, B. (1999). U.S. Military Opportunities: Information Warfare Concepts of Operation. Strategic Appraisal: The Changing Role of Information in Warfare. Santa Monica: RAND Corporation. pp. 179 – 215.

OTAN. (2010). The Global Commons Project. Bruselas: OTAN.

Schreier, F. (2012). On Cyberwar. Ginebra: DCAF, p. 133.

Schwartau, W. (1996). Chaos on the Electronic Superhighway: INFORMATION WARFARE. 2 Ed. New York: Thunder's Mouth. 1996, p. 264.

Sierra Agudelo, G. L. (2011). Me conecto... luego existo: de los efectos de la cibercultura en

la subjetividad, la educación y la familia. Corporación Ser Especial: Medellin.

Taddeo, M. (2012) Information Warfare: a Philosophical Perspective. Philosophy & Technology. Marzo. 25(1) p. 105 - 120.

Tucker, P. (2014. Abril, 1). Inside the Military's New Office for Cyborgs. Defense One. Recuperado de: http://www.defenseone.com/technology/2014/04/inside-militarys-new-office-cyborgs/81670/

Universidad Nacional Autónoma de México (2015). La Cibernética de Cibernética y Computación. Portal Académico. Recuperado de: http://portalacademico.cch.unam.mx/alumno/cibernetica1/unidad1/laCibernetica/introduccion

Upbin, B. (2014. Octubre, 29). First Look At A Darpa-Funded Exoskeleton For Super Soldiers. Forbes Tech. Recuperado de: http://www.forbes.com/sites/bruceupbin/2014/10/29/first-look-at-a-darpa-funded-exoskeleton-for-super-soldiers/

Vallée, R. (2009). HISTORY OF CYBERNETICS. En: Parra-Luna, F. (ed.) SYSTEMS SCIENCE AND CYBERNETICS – Vol. III. (pp. 22 – 34) Encyclopedia of Life Support Systems.

Waterfall, G. (2011). .l E-espionage What risks does your organization face from cyber-attacks? Londres; PricewaterhouseCoopers LLP, p.14.

Wiener, N. (1965). Cybernetics: or the Control and Communication in the Animal and the Machine. Massachusetts: The MIT Press.

Wilson, C. (2004). Information Warfare and Cyberwar: Capabilities and Related Policy Issues. En: CRS Report for Congress. Julio, pp. 3 – 21.

Yakovleff, M. (2014). Battlefield Robotization: Toward a New Combat Ecosystem. En: Robots on the Battlefield Contemporary Issues and Implications for the Future. Fort Leavenworth: Combat Studies Institute Press, pp. 243 – 258.

ESCUELA SUPERIOR DE GUERRA REPÚBLICA DE COLOMBIA

CEESEDEN

Estudios en

SEGURIDAD y DEFENSA

Volumen 10 No. 20 diciembre de 2015

Para solicitar un ejemplar en físico o en formato PDF o para confirmar el acuse de recibo de la revista, por favor escribir a:

Escuela Superior de Guerra
Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacionales
CEESEDEN

Carrera 11 No. 102-50 Teléfono: 620 40 66 Ext.:21455
e-mail: revistaceeseden@esdegue.mil.co
www.esdegue.mil.co

Bogotá - Colombia

ESCUELA SUPERIOR DE GUERRA
COLOMBIA
Fundada en 1909
Unión, Proyección, Liderazgo

Programa en Ciberseguridad y Ciberdefensa

ISO 9001:2008
NTCGP 1000:2009
BUREAU VERITAS
Certification

Escuela Superior de Guerra
Carrera 11 No. 102-50 Bogotá, Colombia
Conmutador 620 4066
www.esdegue.edu.co
programaciber@esdegue.edu.co